REMARKS

This is in response to the Office Action dated September 30, 2008, in which claims 1-35 were rejected. With this Amendment, claims 1-35 have been cancelled and claims 36-62 have been added as new claims in the application. Applicant respectfully requests consideration and allowance of all pending claims.

I. NEW CLAIMS

Newly added independent claim 36 is generally similar to cancelled independent claim 1. However, claim 36 further includes a step of generating a first shared secret key for the second peer with the first public key of the first certificate. Cancelled claim 5 included the use of the first public key of the first certificate in a formula for generating the first shared secret key. The elements of claim 36, which were included in cancelled claim 1, have additionally been altered to generally associate the adjective "first" with the first peer in an effort to make the claim more readable. Support for independent claim 36 can be found, for example, in paragraph 40 of the specification. Newly added independent claim 51 is similar to cancelled independent claim 17 and new independent claim 36. Also, newly added independent claim 57 is similar to new independent claims 36 and 51. Support for the newly added dependent claims can be found, for example, in paragraphs 30, 33 and 40 of the specification. Paragraph 33 indicates that the certificates are created by a trusted third party (certificate authority) that is separate and independent of the two peers.

II. CLAIM REJECTIONS

In section 3 of the Office Action, claims 1-32 were rejected under 35 U.S.C. §103(a) as being unpatentable over Qu et al., U.S. Patent No. 6,792,530 in view of Lenstra, et. al., U.S. Patent No. 7,076,061.

The only section of Qu that provides details regarding the computation of shared keys is column 19, line 6 through column 20, line 7. This section is included below.

> The following examples are illustrated with respect to scheme 3 (or Scheme 7') as CA's signing equation since everyone shares the same generator in this scheme. Each user can have a different CA as long as the CAs use the system parameters (p,q,d) and each user has the same generation.

Setup:

CA1: system parameters (α, β_1, p, q, d)

Alice has a private key a, generator a and publishes (α, I_A, β, γ_A, p, q) in the public domain.

CA2: system parameters (α, β_2, p, q)

Bob has a private key b, a generator α and publishes (α, I_A, β, γ_A, p, q) in the public domain.

We use the MTI/C0 key agreement protocol to demonstrate how to use our new scheme. Assume Alice and Bob want to perform a key exchange. The MTI/C0 protocol

1. Alice reconstructs Bob's public key $\alpha^b = \beta^{F(\gamma_B, I_B)}\gamma_B$, and randomly chooses an integer x and computes $(\alpha^b)^x$, then sends it to Bob.
2. Bob reconstructs Alice's public key $\alpha^a = \beta^{F(\gamma_A, I_A)}\gamma_A$, and randomly chooses an integer y and computes $(\alpha^a)^y$, then sends it to Alice.
3. Alice computes the shared key $K_A = \left(\alpha^{ay}\right)^{xa^{-1}} = \alpha^{xy}$
4. Bob computes the shared key $K_B = \left(\alpha^{bx}\right)^{yb^{-1}} = \alpha^{xy}$

This is a two-pass protocol. With the implicit certificate scheme of the present invention, each party only does three exponentiation operations to get the shared key while at the same time performing an authentication key agreement and implicit public key verification.

Independent claim 36 includes "generating a first shared secret key for the second peer with the first public key of the first certificate." Neither item 3 (Alice's computation of the shared key) nor item 4 (Bob's computation of the shared key) in the above section of Qu shows the generation of a shared secret key with a public key of a certificate. Further, the remaining sections of Qu do not show or expressly or impliedly suggest the above element of claim 36.

Lenstra describes improving key generation and cryptographic applications in public key cryptography, by reducing the bit-length of public keys, thereby reducing the bandwidth requirements of telecommunications devices, such as wireless telephone sets. The teachings of Lenstra do not make up for the deficiencies of Qu.

Yeager relates to distributed trust mechanisms for decentralized networks. Yeager's description of trust mechanisms includes nothing about shared key generation in a manner required by claim 36. Thus, Yeager does not compensate for the deficiencies of Qu and Lenstra.

In view of the foregoing, claim 36 is believed to be allowable over the cited art. Independent claims 51 and 57 have elements similar to those of independent claim 36. Thus, for the same reasons as independent claim 36, Applicant submits that independent claims 51 and 57 are allowable as well. Applicant respectfully submits that the dependent claims are also allowable by virtue of their dependency, either directly or indirectly from the allowable independent claims. Further, the dependent claims set forth numerous elements not shown or suggested in the prior art.

In view of the foregoing, Applicants respectfully request consideration and allowance of claims 36-62. Favorable action upon all claims is solicited.

The Director is authorized to charge any fee deficiency required by this paper or credit any overpayment to Deposit Account No. 23-1123.

Respectfully submitted,

WESTMAN, CHAMPLIN & KELLY, P.A.

By: /Alan G. Rego/

Alan G. Rego, Reg. No. 45,956
900 Second Avenue South, Suite 1400
Minneapolis, Minnesota 55402-3319
Phone: (612) 334-3222 Fax: (612) 334-3312

AGR/dmm